aqua

Community-Driven Cloud Native Security

Using open source software to evolve enterprise-class security solutions

May 2021

Table of Contents

Introduction

While in the midst of a widely recognized shortage of qualified security personnel, the responsibility for software security has undergone a requisite shift “to the left,” raising expectations for developers for the security of the cloud native software they are shipping daily. Amid all this, many organizations are transitioning to DevOps methodologies, with CI/CD pipelines and containerized applications pushing frequent and complex changes to their cloud native software ecosystem.

This simple trend has brought to light one of the most inherent truths of the software supply chain: *Security, development, and DevOps teams work in very different ways*. This, however, does not mean that they must be at odds with each other.

Minimizing the security gap among cloud native applications and DevOps delivery methodologies is a concerted effort that requires input from many stakeholders and the investment of valuable time to establish a clear path forward. For many, this includes a set of tools that satisfy security requirements while empowering developers to exercise their creativity without slowing them down or risk missing a tight shipping deadline – this is commonly summarized as “DevSecOps”. It is at this inflection point between recognizing a need and identifying the solution where many organizations get stuck.

Developers have been using open source components for years, finding open source projects to be a natural way to experience and evaluate new ideas and practices in their own unique ways. Often, this can be done without financial investment and in the safety of developers’ own controlled environments. Now, this approach is rapidly being adopted among developers to explore the use of open source tools to support cloud native security initiatives and avoid the organizational paralysis that often results when applying a top-down security strategy to DevOps methodologies. For the cloud native security experts at Aqua Security, open source has become paramount to their mission to provide enterprise-class security solutions for modern DevSecOps, leading to increased investment and dedicated engineering efforts to a broad portfolio of security-focused open source projects.

How Open Source Fosters Commercial Success

While the value of open source software is largely evident to developer communities and organizations, many might see an overt conflict between open, “free” software solutions and the need for software vendors to provide commercial solutions to stay in business. Considering this, Aqua Security is resolute in two core beliefs:

- Cloud native software security should be achievable, and
- Community-driven innovation can reveal possibilities unseen to software vendors.

The union of these beliefs ultimately yields higher quality software that benefits everyone and democratizes the future of cutting-edge security. Aqua builds upon this to deliver the inherent value of support and insight from a team of cloud native experts dedicated to your specific needs as a customer. Aqua provides its customers with enhanced configuration and security capabilities, and deeper proprietary insight than is possible under an open, community-based solution.

Why We Invest in Open Source

To lower the barrier to entry and to establish a baseline of cloud native security fundamentals for the global community.

Why We Invest in Commercial Solutions

To elevate the standard for cloud native security and help enterprises improve their cloud security risk posture.

We are better equipped to provide dedicated service and support to our customers who lack the resources or expertise to properly secure containerized deployments and cloud native applications on their own. We also emphasize mutual value for a wide array of technology partners, enhancing the effectiveness our commercial solutions via integration and enhancing our partners’ solutions via additional security capabilities. Lastly, open source has consistently proven to yield faster development and higher quality results due to community participation, providing Aqua with direct

insight into true, cutting-edge technological requirements that would take longer to surface in traditional enterprise software implementations.

Ultimately, we believe in the viability of open source solutions for cloud native security for DevSecOps, and we encourage individuals and organizations to explore new security practices by testing out our full portfolio of open source projects. A subset of those who leverage our open source solutions eventually reach a point where they need an integrated, scalable solution built on the open source tools they're familiar with. With extensive integrations, greater usability and functionality, and suitability for use cases from development, through security testing, and into deployment, Aqua Security's commercial solutions elevate the standard for cloud native software security.

What Investing in Open Source Means for Security

In today's DevOps environments, artifacts are constantly being updated and pushed through the pipeline. Amid this rapid change and complexity, organizations must focus their attention on many aspects of security, including facilitating secure development practices (e.g., application security testing, vulnerability scanning), container security and immutability during runtime, and the security of the cloud environments in which these applications and containers are deployed.

Realizing these challenges, open source and cloud native communities have started contributing to projects hosted on GitHub to establish a fertile landscape and foster security solutions for those who are re-architecting their software security programs for a cloud native world. These projects seek to provide new security-focused solutions driven by a community of developers currently emersed in the DevSecOps transition. We at Aqua Security believe we have a mission to extend this fundamental benefit of open source to cloud native security for modern DevOps and remove the barrier to entry for proper security practices.

As a developer and vendor of commercial enterprise security solutions, we have made a conscious decision to invest strategically in open source, in order to:

- Educate individuals and organizations on the best practices for cloud native software development, deployment, and container security,
- Empower a grass roots transformation of legacy security methodologies into DevSecOps and help make security an integral part of the developer's work process,
- Foster community-driven innovation of container security and cloud security solutions, and
- Accelerate adoption of cloud native application methodologies.

We aim to make our open source projects a cohesive and complementary family of cloud native security tools that can provide complementary benefits when used together while also standing on their own to fill a specific gap. Of course, because they are built to satisfy a savvy open source community, our projects put the developer and DevOps first, supporting security needs through the lens of their day-to-day activities. We strive to align the projects we support to the cloud native application lifecycle and threat model, and we resolve to stay focused on maintaining the most powerful and relevant solutions. Through these combined efforts, we are realizing unbridled innovation for security solutions among cloud native developer communities; that is a success in our books.

Aqua's Criteria for Considering OSS Initiatives

We are keenly focused on enhancing cloud native and container security and we are resolute in making DevOps security achievable. To help achieve these goals, Aqua has established an internal team of developers focused on the open source projects we own and maintain as well as collaborating outside our own projects. This team is a team of developers and security problem solvers, who align to a clear and objective set of criteria in order to prioritize their efforts. This includes:

Relevance

To engender the idea of cloud native security for everyone, we contribute what we know best: security for containerized deployments atop common open source platforms within the most popular clouds. To ensure alignment between our open source projects and our full-featured, commercially available solutions, we maintain projects to help secure the build, to secure the infrastructure, and to secure the running workload. These three pillars of cloud native security are fundamental to the success of a modern DevSecOps program, with each pillar depending on the success of another, and are paramount to our investment in open source.

Impact

We also evaluate the potential reach and influence the project can have on the community, working to improve the security risk posture of as many individuals and organizations as possible. This metric considers the variety of development and deployment methodologies, underlying technologies, and the range of potential use cases. Yes, we are a solution vendor, and we are also members of the broader software community; we do not believe security should be relegated only to those who choose to partner with us commercially. It is as simple as that.

Sustainability

This criterion aggregates the previous two and poses one crucial question: *Can we support this project over time, and can community engagement endure?* We seek to maintain impact and relevance over time to ensure the benefits derived from open source collaboration continue to be realized. If a project's sustainability is low, then impact or relevance can be adversely affected depending on technological or community changes.

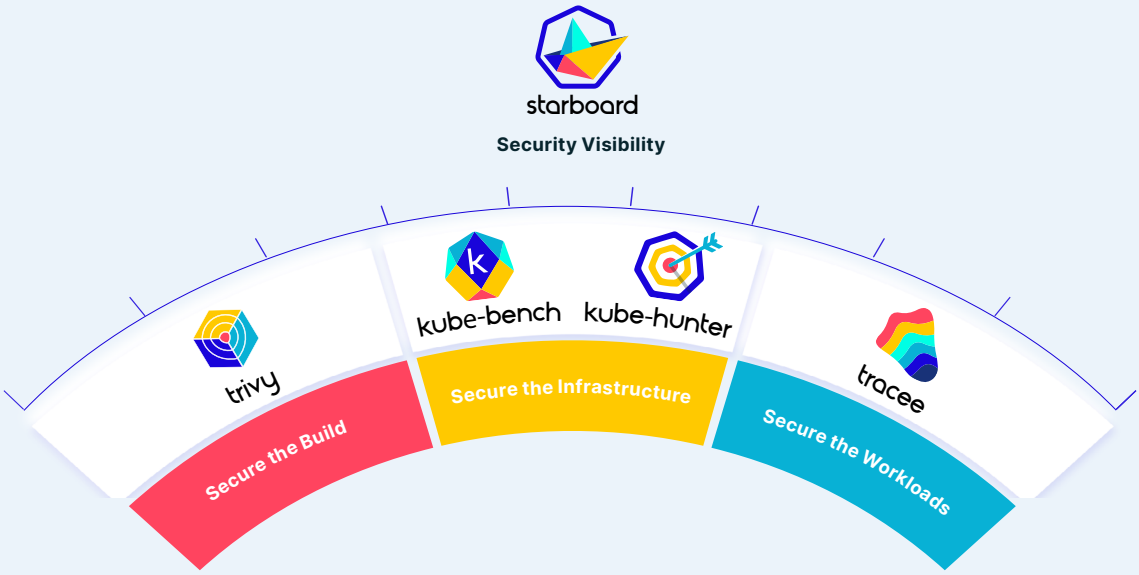
Roadmap

While we are experienced security and DevSecOps practitioners, we believe wholly that there is much to be learned from open exchange of ideas as facilitated through open source development. Our choice to maintain or engage in a project is also influenced by its potential for learning and how we might leverage it to evolve our commercial solutions. In essence, we wish to derive benefit for our engineering teams as well as our customers when we learn from the very communities we support.

Cloud Native Security, the Open Source Way

Calling back to the three key pillars of cloud native security - securing the build, securing the infrastructure, and securing the running workload – Aqua is focused on helping organizations to do so as efficiently as possible. We own, maintain, contribute to, and curate a powerful open source portfolio to address these areas. As part of our commitment to open innovation, we have licensed many of the projects we own under the permissive Apache 2.0 license. Under this license, these projects are also capable of greater interplay with other projects and solutions, ultimately increasing their potential reach and influence.

Supporting Cloud Native Security with Open Source



Trivy detects vulnerabilities (e.g., CVEs) in open source software and provides a brief explanation of risk so developers can make more informed decisions regarding the components they incorporate into their applications and containers to secure the application before it ships. While many developers' container security protocol already involves some sort of static image scan for vulnerabilities, this usually occurs after code editing has finished. Because of this, we enabled Trivy to seamlessly merge vulnerability scanning into the Integrated Development Environment (IDE).

Progressing beyond the IDE into container registries and the endpoint of the CI pipeline, Trivy is also the first scanner with a plug-in adapter for the Harbor registry and has been chosen as the default scanner from Harbor version 2.0 onwards, following positive feedback from the community. Open source contributors have also been working to create integrations and add-ons for Trivy, such as a Prometheus exporter for extracting vulnerability metrics, and a Helm chart for installing Trivy into a Kubernetes cluster.

Fun Fact

Aqua is combining the best of both worlds, incorporating Trivy into aspects of our commercial solutions. Where Trivy collects vulnerability data from different security advisory distros, package managers, and language security advisory locations, our commercial Aqua solutions augment Trivy with additional information and functionality for customers like support for multi-tenancy, SSO, high-value threat intelligence, the ability to scan for secrets and to perform malware scanning, and more.

Harbor is an open source cloud native artifact registry, initiated by VMware and governed by the Cloud Native Computing Foundation (CNCF). Harbor can be used as a repository for container images and leverages contributions from Aqua to provide support for vulnerability scanning of images to ensure their safety for deployment. Aqua has been collaborating with the Harbor community to extend its capabilities with support for pluggable image vulnerability scanners like Trivy. Trivy can also be set as the default scanner when deploying Harbor for faster risk evaluation.

Pro Tip

Whether you choose to explore cloud native security in Harbor using the open source Trivy scanner or to experience some of the additional functions included with the commercially available Aqua CSP scanner, be sure to enable the scanning capability on your Harbor instance.

aqua kube-bench

Kube-bench is a Kubernetes configuration security checker, helping to secure the infrastructure for cloud native application deployment. This project provides a way to test a Kubernetes cluster to see if it complies with the CIS Kubernetes benchmark, identifying whether a cluster is configured based on security best practices. Since this project's inception, Aqua has also created other benchmark projects, including our own versions of Docker-bench and Linux-bench.

Community participation has helped Kube-bench evolve rapidly, with contributions that have enabled tests to run across many different platforms, provided node type detection capabilities, and more. This has fostered broader adoption and lowered the barrier to entry.

Fun Fact

As with other innovative open source projects, the community has also helped immensely with bug resolution and contributions to the documentation. Such have greatly improved the overall quality and user experience of Kube-bench.

aqua kube-hunter

Kube-hunter is an open source penetration testing tool for Kubernetes that compliments the CIS benchmark-based approach offered by Kube-bench. While not strictly a traditional pen-testing tool, Kube-hunter helps detect potential security risks or bad configuration issues in the Kubernetes cluster. Kube-hunter does what an attacker would do, looking for potential entry points or weaknesses which could be exploited. Kube-hunter's real strength is the flexible architecture

where community developers can contribute their custom-coded “hunters,” which try to perform different security tests. Many of these tests are documented via the Kube-hunter website.

Fun Fact

Once detected, Kube-hunter reports this information and provides remediation advice on which appropriate actions can be taken to close the gaps and improve security. Kube-hunter’s reports provide insight into an array of issues and risk criteria, , detailing Risk Category, Vulnerability Type, Risk Description, and Evidence.

Tracee is a lightweight and easy-to-use container and system-tracing tool, implemented using eBPF, that enables users to improve runtime security for cloud native workloads. Tracee runs the container and observes system calls and other system events in real time. In addition to collecting raw system events, Tracee provides additional security insights, such as files written to disk or to memory, files that were executed during the trace lifetime, or extract binaries that are dynamically loaded to an application’s memory. This diverse set of capabilities enables users to quickly gain insight into the running container. Tracee is also the engine behind Aqua’s commercial Dynamic Threat Analysis (DTA) solution.

Perhaps one of Aqua Security’s most ambitious open source projects, Starboard is a toolkit for finding risks in your Kubernetes workloads and environments. Starboard draws its origins from the challenge of having to learn a new interface and deployment for each new tool. In essence, Starboard is a Kubernetes-native security toolkit, taking a vendor-agnostic approach to extracting results from a variety of tools from Aqua and other third-party projects and making them available in a Kubernetes-native way.

Starboard enables results from vulnerability scanners, workload auditors, and configuration benchmark tests to be incorporated into Kubernetes custom resource

definitions (CRDs) and accessed through the Kubernetes API. This means you can run solutions of your choice, integrate them into Kubernetes, and consume or compare their reports in the same location.

Aqua's motivation for maintaining Starboard is straightforward: *It's not easy to deal with the results from these different, standalone Kubernetes security tools*. Starboard attempts to benefit the cloud native security ecosystem by establishing a schema for a vulnerability, a risk assessment check, an allowed or denied vulnerability, or a scanner configuration.

Aqua has aligned Starboard to three key use cases, providing organizations a clear path of progression into more comprehensive commercial solutions as they mature beyond open source. These include:

- Security toolkit for development teams to shift security left,
- Security toolkit for enterprise DevOps by creating an operator to improve automation, policy enforcement, and scalability,
- Security product development toolkit for security vendors and internal dev teams by enabling the reuse of one of the existing CRDs for the results.

Fun Fact

By aggregating results into an overview of current security status, security vendors can focus on what they do best while users can efficiently manage diverse assessments and consume otherwise distinct data in the homogeneous format.

Cloud Native Security Gaining Traction in Open Source Communities

Open source projects, regardless of their function, are the result of the creativity, consideration, and feedback of a diverse community of developers. The suite of cloud native and container security projects backed by Aqua Security is no different. When evaluating a project's traction among the community, it is important to understand the metric upon which traction is measured.

Consumption can help measure a project's reach within the community and can be used to approximate the potential influence of the project when it is implemented. Engagement can help evaluate the degree to which those who consume the project are inspired to give back to the community, and can be broken out into categories of feedback (e.g., satisfaction, recommendations) and contribution (e.g., pull requests, forks).

As a project's traction begins to grow, it is important to consider additional factors which can help accelerate that growth. Among the most influential of these factors is increasing usability and lowering barriers to entry. Aqua's open source team attempts to remove friction wherever possible, like investing in improvements to the documentation, and encourages the community to help fill the gaps.

Aqua Security and the CNCF

Aqua's deep involvement with the CNCF is all about community, engaging directly to solve issues and to extract valuable insight from the very groups we seek to support. The CNCF provides a neutral ground for people to collaborate on cloud native projects. Through this involvement, we work to establish an informed and strategic direction for the community's activities.

Our dedicated team of open source developers are deeply invested in the success and evolution of the projects sponsored by the CNCF. Members of our open source engineering team have held – or continue to hold – positions with the CNCF, including Technical Oversight Committee (TOC) Chair and CNCF Ambassador. Members of the team also maintain other CNCF projects, co-chair industry events, organize regional CNCF meetups, and author educational books and certification exams.

This concerted effort ensures a project's relevance to the goal of enhancing security for cloud native stacks and fostering broader adoption of cloud native technologies, methodologies, and mindsets. The CNCF TOC is keenly focused on the greater good, often serving as a feedback loop for projects and maintainers who are having difficulty overcoming a challenge for their own customers and audience.

In keeping with the core values of the Linux Foundation, Aqua's contributions to the cloud native community and its engagement with the CNCF extends the goal of making Kubernetes technologies easy-to-use with a communal responsibility for their adoption and evolution. By maintaining cloud native security solutions in an open source format Aqua has placed great emphasis on the importance of trust to community developers and security professionals.

For more information on Aqua Security's portfolio of open source and commercial solutions for cloud native software security, visit: